**Modern Studies in Management & Organization**
**Volume 1, Issue 4 - Winter 2025 - Pages 75-92**
Homepage: https://www.jmsmo.ir

# The Effect of Institutional Theory Dimensions on Information Security Management Based on ISO 27001 (Study of: Shahrekord Medical Sciences Teaching Hospitals)

**Roh Allah Kargar Boldaji [1], Mohammad Javad Salehpour [2]***

1. Department of management, Deh.C, Islamic Azad University, Isfahan, Iran.
2. Department of management, Deh.C, Islamic Azad University, Isfahan, Iran.

**OPEN ACCESS**

**Article type:** Research Article

***Correspondence:** Mohammad Javad Salehpour
mjsalehpour@gmail.com

**Received:** October 20, 2024
**Accepted:** February 26, 2025
**Published:** Winter 2025

**Citation:** Kargar Boldaji, R. A., Salehpour, M. J. (2025). The Effect of Institutional Theory Dimensions on Information Security Management Based on ISO 27001 (Study of: Shahrekord Medical Sciences Teaching Hospitals). Modern Studies in Management & Organization, 1(2), 75-92.

**Publisher's Note:** JMSMO stays neutral with regard to jurisdictional claims in published material and institutional affiliations.



**Abstract:** The present study aimed to investigate the effect of institutional theory dimensions on information security management based on ISO 27001 in Shahrekord Medical Sciences Teaching Hospitals, which was conducted using a descriptive-correlation method. The study's statistical population included Shahrekord hospitals, which consisted of 10 hospitals and 3 clinics, of which hospital information technology experts were surveyed using a census method. After distributing 48 questionnaires, 45 completed questionnaires were finally obtained, and the questionnaire data were analyzed. The research variables were measured using the standard questionnaire of Cavusoglu et al. (2015) and the Security Management System Quality Assessment Questionnaire using ISO 27001. The variables in the questionnaire were measured on a five-point Likert scale. Data analysis was performed at two levels: descriptive statistics using SPSS software and inferential statistics using partial least squares using SmartPLS software. The results of the findings from the analysis of research data showed that the two components of imitative and normative pressure with coefficients of 0.25 and 0.32 had a positive and significant effect on information security management and were able to explain and predict 62% of the changes in information security management in teaching hospitals of Shahrekord University of Medical Sciences.

**Keywords:** Institutional Pressures, Information Security, ISO27001, Hospitals and Educational Medical Centers in Shahrekord.
DOI: 10.22034/jmsmo.2025.221002

## Extended Abstract

### Introduction

Today, information plays a role similar to that of an organization's capital, and protecting its information is one of the most important pillars of its survival. The information security management system defines information protection in three specific concepts: information confidentiality, information integrity, and information availability. Many failures in implementing information security management stem

from organizational issues and a lack of attention to the organization's readiness before implementation. In 2005, one of the most comprehensive information security management system standards was developed, ISO 2005: 27001. The purpose of developing this national standard was to specify the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, improving, and promoting a documented information security management system, taking into account the concept of the organization's macro-business risks. One of the features of this standard is the existence of 113 security controls in the form of 35 control objectives and 14 areas including the organization's security policy, asset management, human resource security, physical and environmental security, operational security, communication security, access control, encryption, supplier relations, acquisition, development and maintenance of information systems, information security incident management, business continuity management and compliance, which cover various managerial, operational and technical aspects in an organization. According to another feature (security management approach based on institutional historical theory), there should be a balance between information protection and authorized access. The important point is that information security should be managed at all organizational levels (strategic, tactical, and operational) and the necessary controls should be implemented (Parks et al., 2011).

**Theoretical framework**

Institutional theory is one of the most valid theories to explain the relationship between an organization and its environment, which has gained great credibility among researchers since the early 1980s. The main issue in institutional theory is the "conformity of organizations" in the face of institutional pressures, which results in gaining legitimacy for the organization, and information security means protecting information and information systems from unauthorized activities. These activities include access, use, disclosure, reading, copying or recording, destruction, modification, and manipulation. The main objectives of an information security policy can be divided into three parts: confidentiality (ensuring that information is only in the hands of authorized individuals), integrity (protecting information from change, distortion, and destruction), and availability (ensuring that information and information systems are available and usable when needed) (Singh et al., 2014).

Imitation pressure causes organizations to imitate actions taken by others, such as competitors, without careful consideration. Organizations often closely monitor the successful actions and methods used by others in their industry. As a result, these successes are used by others as a basis for imitation (Kahooei & Abbasi, 2015). Coercive pressure refers to the fact that organizations are subject to pressures exerted by other organizations and cultural expectations. For example, regulatory authorities may, in some cases, exert direct pressure on an organization by mandating certain organizational practices. Even without directly attempting to influence a company, specific strategic actions taken by influential organizations in an industry may increase indirect pressure on other organizations in that industry (Tseng, 2008). Homogeneity among organizations over time is partly attributed to organizations' compliance with normative pressure. Firms are likely to adjust their behavior based on their beliefs about what is considered appropriate among social groups and, as a result, adopt methods and techniques that reflect the current standards of those groups. Normative pressure can come from a variety of sources, such as business partners and professional associations. Because firms within a value chain generally pursue common goals, a

firm is subject to normative pressure from other members of the value chain. (Siponen & Vance, 2014).

## Methodology

The present study is applied in terms of its purpose, as it seeks to investigate a real problem and provide specialized knowledge, and its results and findings can be used by managers in developing relevant information security controls. In terms of data collection method, it is descriptive and correlational, which is in line with the objectives and hypotheses of this study. Therefore, the present study is applied in terms of purpose because it examines the impact of institutional theory dimensions on information security control resources, and in terms of data collection and analysis method, this study is descriptive and correlational. Also, in terms of time, this study is cross-sectional. The statistical population of this study is all clinics and teaching hospitals of Shahrekord University of Medical Sciences, 10 hospitals and 3 clinics, and the level of analysis is the organization. The analysis of the results of this study was conducted using SPSS and Smart PLS statistical software at two levels of descriptive and inferential statistics. In the descriptive statistics section, statistical characteristics such as frequency, percentage, mean, and standard deviation were used, and in the inferential statistics section, structural equations (partial least squares method) were used.

## Discussion and Results

In this study, the effect of institutional theory dimensions on information security management in teaching hospitals of Shahrekord University of Medical Sciences was determined. Accordingly, an attempt was made to initially identify the components related to each variable based on theoretical literature and research background, and then the research model resulting from the effect of institutional theory dimensions on information security management was drawn. The statistical population of the study included all teaching clinics and hospitals of Shahrekord University of Medical Sciences, 10 hospitals, and 3 clinics. Questionnaires were distributed among all employees of the information technology units of hospitals and teaching clinics of Shahrekord University of Medical Sciences, and finally, 45 questionnaires were collected. The average scores of each hospital and clinic were calculated and used as final data for analysis. The questionnaires were prepared and localized through a standard questionnaire. To measure the dimensions of institutional theory, the questionnaire of Kavsgulu et al. (2015) was used, and to measure information security management, the ISO 27001 questionnaire was used. The face validity of the questionnaires was confirmed by the supervisor, and the content validity was confirmed by the professors of the management group and a number of members of the statistical sample. After that, the construct validity was confirmed using convergent and divergent validity indices, and the reliability of the questionnaire was confirmed by composite reliability indices and Cronbach's alpha and factor loadings.

The variables in the questionnaire were measured on a five-point Likert scale. Data analysis was performed at two levels of descriptive statistics and inferential statistics through internal and external models using Smart PLS software. The results of the findings from the analysis of the research hypotheses showed that the two dimensions of coercive and normative pressure have the ability to predict 62% of security management in teaching hospitals of Shahrekord University of Medical Sciences.

## Conclusion

In today's interconnected e-business environment, concerns about security are growing. The use of information technology carries special risks for information systems, especially vital and important resources, due to its nature. For this reason, today, many organizations are seeking to create security systems to prevent their information from leaking out in order to protect their entire collection. Information system security is like a chain whose strengths are affected by weaknesses. Shahrekord University of Medical Sciences, as a government organization, maintains a large volume of information in the systems available in the organization, which requires high protection as it is related to personal, educational, and professional information of individuals. We must ensure that all risks are formally identified, ranked, monitored, and their occurrence is prevented or their impact is reduced. In the present study, an attempt was made to evaluate the status of information security management in each dimension in the information technology departments of Shahrekord University of Medical Sciences using the ISO/27001 standard. In order to analyze the secondary question, considering the use of the census method, the average method was used. Since the average of all dimensions exceeded 3, it can be concluded that the status of information security management in the educational medical centers of Shahrekord University of Medical Sciences is in a favorable state, according to the information technology experts of these centers.

## Contribution of authors

All authors have participated in this research in equal proportion.

## Ethical approval

Written informed consent was obtained from the individuals for their anonymized information to be published in this article.

## Conflict of interest

No conflicts of interest are declared by the authors.

# مطالعــات نوین در مدیریت و سازمان

**سال اول، شماره چهارم، زمستان ۱۴۰۳ – صفحه ۹۲-۷۵**

Homepage: https://www.jmsmo.ir


# تأثیر ابعاد تئوری نهادی بر مدیریت امنیت اطلاعات بر مبنای ایزو ۲۷۰۰۱ (مورد مطالعه: بیمارستان‌های آموزشی علوم پزشکی شهرکرد)


**روح الله کارگر بلداجی [۱]، محمد جواد صالح پور [۲*]**

۱. گروه مدیریت، واحد دهاقان، دانشگاه آزاد اسلامی، اصفهان، ایران.

۲. گروه مدیریت، واحد دهاقان، دانشگاه آزاد اسلامی، اصفهان، ایران.



**چکیده:** هدف پژوهش حاضر، بررسی تأثیر ابعاد تئوری نهادی بر مدیریت امنیت اطلاعات بر مبنای ایزو ۲۷۰۰۱ در بیمارستان‌های آموزشی علوم پزشکی شهرکرد بود که به روش توصیفی-همبستگی صورت گرفته است. جامعه آماری پژوهش شامل بیمارستان‌های شهرکرد بوده که تعداد آن‌ها ۱۰ بیمارستان و۳ کلینیک بود، که از این میان به روش سرشماری از کارشناسان فناوری اطلاعات بیمارستان‌ها نظرخواهی شد. پس از توزیع ۴۸ پرسشنامه، در نهایت ۴۵ پرسشنامه تکمیل شده بدست آمد و داده‌های پرسشنامه مورد بررسی قرار گرفت. متغیرهای پژوهش با استفاده از پرسشنامه استاندارد کاواسوگلو وهمکاران (۲۰۱۵) و پرسشنامه ارزیابی کیفیت سیستم مدیریت امنیت با استفاده از ایزو ۲۷۰۰۱ سنجیده شد. سنجش متغیرها در پرسشنامه درطیف پنج درجه‌ای لیکرت صورت پذیرفت. تجزیه وتحلیل داده‌ها در دو سطح آمار توصیفی با نرم افزار SPSS و آمار استنباطی ازطریق حداقل مربعات جزئی توسط نرم افزار SMARTPLS صورت پذیرفت. نتایج یافته‌های حاصل از تجزیه و تحلیل داده‌های پژوهش نشان داد که دو مؤلفه فشار تقلیدی و هنجاری با ضرایب ۰/۲۵ و ۰/۳۲ تأثیر مثبت و معناداری بر مدیریت امنیت اطلاعات داشته و توانسته‌اند ۶۲ ٪ از تغییرات مدیریت امنیت اطلاعات در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد را تبیین و پیش‌بینی کنند.



**واژگان کلیدی: فشارهای نهادی، امنیت اطلاعات ، ISO27001، بیمارستان‌ها و مراکز درمانی آموزشی شهرکرد.**

DOI: 10.22034/jmsmo.2025.221002

**دسترسی آزاد**

**نوع مقاله:** مقاله پژوهشی



***نویسنده مسئول:** محمد جواد صالح‌پور

mjsalehpour@gmail.com



**تاریخ دریافت:** ۱۴۰۳/۰۷/۲۹

**تاریخ پذیرش:** ۱۴۰۳/۱۲/۰۸

**تاریخ انتشار:** زمستان ۱۴۰۳

**استناد:** کارگر بلداجی، روح‌الله و صالح‌پور، محمد جواد. (۱۴۰۳). تأثیر ابعاد تئوری نهادی بر مدیریت امنیت اطلاعات بر مبنای ایزو ۲۷۰۰۱ (مورد مطالعه: بیمارستان‌های آموزشی علوم پزشکی شهرکرد). فصلنامه مطالعات نوین در مدیریت و سازمان، ۲(۱)، ۹۲-۷۵.

**یادداشت ناشر:** JMSMO درخصوص ادعاهای قضایی در مطالب منتشر شده و وابستگی‌های سازمانی بی‌طرف می‌ماند.




## مقدمه

امروزه، اطلاعات نقش سرمایهٔ یک سازمان را ایفا می‌کند و حفاظت از اطلاعات سازمان یکی از ارکان مهم بقای آن است. سیستم مدیریت امنیت اطلاعات، حفاظت از اطلاعات را در سه مفهوم خاص محرمانه بودن اطلاعات، صحت اطلاعات و در دسترس بودن اطلاعات تعریف می‌کند. بسیاری از شکست‌های پیاده‌سازی مدیریت

امنیت اطلاعات ریشه در مسائل سازمانی و بی‌توجهی به وضعیت آمادگی سازمان قبل از پیاده‌سازی دارد. در سال ۲۰۰۵ یکی از جامع‌ترین استانداردهای سیستم مدیریت امنیت اطلاعات با نام ایزو ۲۰۰۵: ۲۷۰۰۱ تدوین شد. هدف از تدوین این استاندارد ملی، مشخص کردن الزامی برای ایجاد، اجرا، بهره برداری، پایش، بازنگری، نگهداری، بهبود و ارتقای یک سیستم مدیریت امنیت اطلاعات مستند شده، با در نظر گرفتن مفهوم ریسک‌های کلان کسب وکار سازمان بود. از ویژگی‌های این استاندارد، وجود ۱۱۳ کنترل امنیتی در قالب ۳۵ هدف کنترلی و ۱۴ حوزه شامل خط‌مشی امنیتی سازمان، مدیریت دارایی، امنیت منابع انسانی، امنیت فیزیکی و محیطی، امنیت عملیات، امنیت ارتباطات، کنترل دسترسی، رمزنگاری، ارتباط با تأمین کنندگان، اکتساب، توسعه و نگهداری سیستم‌های اطلاعاتی، مدیریت حوادث امنیت اطلاعات، مدیریت تداوم کسب وکار و انطباق است که جنبه‌های گوناگون مدیریتی، عملیاتی و فنی را در یک سازمان پوشش می‌دهد. براساس ویژگی دیگر آن (رویکرد مدیریت امنیت براساس تئوری تاریخی نهادی)، باید تعادلی میان حفاظت اطلاعات و دسترسی مجاز باشد. نکتهٔ مهم این است که امنیت اطلاعات باید در تمام سطح سازمانی (راهبردی، تاکتیکی و عملیاتی) مدیریت شود وکنترل‌های لازم پیاده سازی شوند (Parks et al., 2011).

امروزه، بیمارستان‌ها تلاش می‌کنند تا برای رقابت با بیمارستان‌های دیگر و کسب نمره قابل قبول در ممیزی‌ها، رضایت بیماران را کسب کنند. در سال‌های اخیر این سازمان‌ها برای ارائه خدمات به مشتریان خود استفاده از پیشرفته‌ترین دستاوردهای علوم مختلف را آغاز کرده‌اند. هدف سازمان‌های مراقبت بهداشتی از بکارگیری این دستاوردها و کاربرد سیستم‌های مراقبت سلامت، بهبود روندکاری، کاهش هزینه‌ها و در نهایت ارتقاء کیفیت خدمات مراقبتی می‌باشد (Das & Mukhopadhyay, 2012).

با پیشرفت‌های اخیر در فناوری اطلاعات و ارتباطات و به منظور ارتقاء کیفیت و سرعت ارائه خدمات به بیماران، مدیریت امنیت فناوری در بخش درمان به عنوان راهکاری جدید برای دسترسی برابر بیماران به مراقبت‌های پزشکی مطرح گردیده است (Guillen et al., 2010). در واقع، از آنجا که امنیت فناوری متکی بر انتقال داده‌ها است، حفظ امنیت شبکه به منظور محرمانه نگاه داشتن انتقال داده‌ها و حفظ حریم خصوصی بیماران امری حیاتی است و هرگونه احتمال تهدید یا حمله به شبکه‌های پزشکی از راه دور، از قبیل ورود افراد غیرمجاز به شبکه و تغییر یا تخریب داده‌های بیماران، باید مورد بررسی قرار گیرد. به عبارت دیگر، هرگونه ضعف در هر بخشی از شبکه پزشکی از راه دور می‌تواند کل سیستم را تحت تأثیر قرار دهد. بنابراین، برای ایجاد مدیریت امنیت اطلاعات در زمینه ذخیره و تبادل اطلاعات در شبکه پزشکی از راه دور باید ساز وکارهای لازم با استفاده از استانداردهای مرتبط مدنظر قرار گیرد (Tallon & Pinsonnault, 2011).

به دلیل شرایط خاص جغرافیایی و اقتصادی استان چهارمحال و بختیاری، به نظر می‌رسد این استان در حوزه فناوی و از جمله مدیریت امنیت اطلاعات در بیمارستان‌ها، از برخی استان‌های پیشروی کشور عقب افتاده است. بنابراین، مطالعه میزان پیاده سازی مدیریت امنیت اطاعات در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد و همچنین تأثیر عوامل درونی و بیرونی بر این پیاده‌سازی بر مبنای نظریه نهادی ضروری به نظر می‌رسد.

طبق بررسی‌های انجام شده در منابع داخلی، تحقیقات متعددی به بررسی مدیریت امنیت اطلاعات پرداخته‌اند؛ ولی با توجه به نوع ساختاری که در اکثر بیمارستان‌های علوم پزشکی حاکم می‌باشد، رویکرد جدی به مقوله امنیت اطلاعات ندارد و در اکثر بخش‌ها همان تفکر سنتی دیده می‌شود. با اینحال فرایند پژوهشی در این تحقیق می‌تواند فضای موجود را در این سازمان با عنایت به متغیرهای ذکر شده تغییر دهد و باعث توسعه اثربخشی سازمانی مدیریت امنیت اطلاعات در این بیمارستان گردد.

علیرغم استفاده بسیاری از سازمان‌ها از استانداردهای امنیت اطلاعات (ISO27000)، مطالعات چندانی در حوزه بیمارستان‌های آموزشی کشور انجام نشده است و نویسندگان فقط یک مطالعه در خصوص ارزیابی سطح امنیت اطلاعات بیمارستان‌ها بر اساس استاندارد امنیت اطلاعات ISO27000 یافتند (Sheikh Abu Masoudi et al., 2015) که مطالعه آنها در دانشگاه علوم پرشکی اصفهان انجام پذیرفته و در نتیجه وضعیت گزارشی پیرامون وضعیت مدیریت امنیت اطلاعات در مراکز درمانی وابسته به دانشگاه علوم پزشکی شهرکرد یافت نشد. علاوه بر این، کاهویی و عباسی (۱۳۹۴) در پژوهشی عوامل مؤثر بر امنیت اطلاعات سلامت سازمانی و رفتاری را به عنوان مهم‌ترین عامل معرفی کردند. همچنین، برگزاری دوره‌های آموزشی، سرمایه‌گذاری فنی و ایجاد زیرساخت فنی از اهمیت بالایی برخوردار بود ( Kahooei & Abbasi, 2015). عیسی زاده (۱۳۹۴) عوامل فناوری، عوامل برون سازمانی و درون سازمانی را به عنوان عوامل کلیدی موفقیت در پیاده‌سازی مدیریت امنیت اطلاعات در اداره کل بنادر و دریانوردی استان گیلان معرفی کردند (Eissazadeh, 2015). تاج فر و همکاران (۱۳۹۳) مهم‌ترین مانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات را ناهمخوانی ساختار سازمانی با ISMS وترس کارکنان از سخت شدن فرآیندهای ناشی از پیاده‌سازی سیستم مدیریت امنیت اطلاعات گزارش کرده‌اند (Tajfar, 2014). مهرآیین و همکاران (۱۳۹۲) وضعیت امنیت اطلاعات را در بیمارستان‌های وابسته به دانشگاه علوم پزشکی تهران و شهید بهشتی بررسی کردند که وضعیت امنیت اطلاعات را قابل قبول گزارش کردند (Mehraeen et al., 2014). شیخ ابومسعودی و همکاران (۱۳۹۴) امنیت محیطی و فیزیکی، مدیریت حوادث امنیت اطلاعات و کنترل دسترسی را در فرآیند مدیریت امنیت اطلاعات بیمارستان‌های علوم پزشکی اصفهان از وضعیت مطلوب‌تری گزارش کردند. رویکرد این پژوهش نسبت به تحقیقات گذشته این است که در این پژوهش انواع سیستم مدیریت امینت اطلاعات، بررسی و به پیش نیازها و الزومات تئوری نهادی خصوصاً در حوزه امنیت اطلاعات توجه می‌شود (Sheikh Abu Masoudi et al., 2015).

نتایج این تحقیق می‌تواند مدیران را در برنامه‌ریزی و مشخص کردن راه آینده در مقابل تغییرات و تحولات امنیت اطلاعات راهنمایی و کمک نماید. همچنین، نتایج این تحقیق می‌تواند با ارایه راهکارهای عملی برای بهبود اثربخشی سازمانی اطلاعات سازمانی مفید واقع شود. به علاوه، نتایج حاصل از پژوهش حاضر می‌تواند در ارائه راهبردهای کاربردی برای ارتقای بیش از پیش مدیریت اثربخشی امنیت اطلاعات و توان علمی و عملی مدیران راهگشا باشد. هدف اصلی این تحقیق، تعیین تأثیر ابعاد تئوری نهادی بر مدیریت امنیت اطلاعات در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد می‌باشد.

## مبانی نظری و پیشینه پژوهش

نظریه نهادی، یکی از معتبرترین نظریه‌ها در باب تبیین ارتباط میان سازمان و محیط آن است که از اوایل دهه ۱۹۸۰ به بعد در میان محققان اعتبار زیادی را کسب کرده است. مسئله اصلی در نظریه نهادی «هم‌شکل شدن سازمان‌ها» در مقابل فشارهای نهادی است؛ که نتیجه آن کسب مشروعیت برای سازمان است و امنیت اطلاعات یعنی محافظت کردن از اطلاعات و سیستم‌های اطلاعاتی از فعالیت‌های غیرمجاز. این فعالیت‌ها عبارتند از دسترسی، استفاده، فاش کردن، خواندن، کپی یا ضبط، خرابکاری، تغییر، دستکاری . اهداف اصلی یک سیاست امنیت اطلاعات را می‌شود به سه بخش محرمانگی (اطمینان از اینکه اطلاعات تنها در دستان افراد مجاز قرار می‌گیرند)، درستی (حفاظت از اطلاعات در مقابل تغییر، تحریف و نابودی)، و دسترس پذیری (اطمینان از اینکه اطلاعات و سیستم‌های اطلاعاتی در زمان مورد نیاز در دسترس و قابل استفاده هستند) تقسیم نمود (Singh et al., 2014).

### فشار تقلیدی

فشار تقلیدی موجب می‌شود که سازمان‌ها از اقدامات اتخاذ شده توسط دیگران مثل رقبا، را بدون تأمل دقیق تقلید کنند. سازمان‌ها اغلب به طور دقیق اقدامات و روش‌های موفق به کار رفته توسط دیگران در صنعت خودشان را نظارت می‌کنند. در نتیجه این موفقیت‌ها توسط دیگران به عنوان اساس تقلید به کار می‌روند. در مواجهه با سطح بالایی از تردید درباره نتایج دوره خاصی از فعالیت‌ها ممکن است سازمان‌ها از طریق پیروی از اقدامات جمعی سیاستگذاران اولیه و اقدامات اتخاذ شده توسط سازمان‌های مشابه به مشروعیت برسند. چنین رفتاری تقلیدی تلقی می‌شود، به خصوص وقتی که سازمان‌ها با مشکلاتی مشابه مواجه می‌شوند و درباره نتایج مورد انتظار دارایی‌های سازمانی برای پرداختن به مشکل توضیحی نمی‌دهند. در دستور العمل IS، نقش فشار تقلیدی برای درک انگیزه‌های سازمانی به منظور استفاده کردن از گونه‌هایی از اقدامات مرتبط به IS مورد بررسی قرار گرفته است. به علاوه، گرچه تحقیقات قبلی تحت عنوان فشار تقلیدی بررسی نشده‌اند، ولی این تحقیقات نشان داده‌اند که تصمیمات مرتبط با فناوری اطلاعات اغلب تقلیدی از اقدامات جمعی اتخاذ شده توسط دیگران در آن صنعت هستند (Kahouei & Abbasi, 2015). به همین نحو انتظار می‌رود که سازمان‌ها اغلب نگران این باشند که هزینه‌های آنها برروی امنیت سیستم‌های اطلاعاتی همسو با هزینه‌های رقبای آنها هستند یا خیر. بنابراین ما فرضیه زیر را مطرح می‌کنیم:

- فشار تقلیدی بر مدیریت امنیت اطلاعات در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد تأثیر دارد.

### فشار اجباری

فشار اجباری اشاره به این دارد که سازمان‌ها در معرض فشارهای اعمال شده توسط دیگر سازمان‌ها و انتظارات فرهنگی هستند. برای مثال، مراکز نظارتی ممکن است در مواردی با دستور دادن شیوه‌های خاص سازمانی فشار مستقیمی بر آن سازمان اعمال کنند. حتی بدون تلاش مستقیم برای تأثیر گذاری بروی یک شرکت، اقدامات استراتژیک

خاص اتخاذ شده توسط سازمان‌های با نفوذ در یک صنعت ممکن است موجب بالا رفتن فشار غیرمستقیم بر دیگر سازمان‌ها در آن صنعت شود. قوانین تحمیلی مانند قانون مدیریت امنیت اطلاعات فدرال و دستورالعمل‌های حفاظت اطلاعات اتحادیه اروپا نمونه‌های قابل توجهی از فشارهای اجباری هستند که سازمان‌ها در امنیت اطلاعات با آن‌ها مواجه می‌شوند. یک تحقیق تازه نشان می‌دهد که تطابق با آیین نامه‌ها موثرترین محرک برای اقدامات امنیت اطلاعاتی سازمان‌ها است. امروزه شرکت‌ها نه تنها باید با قوانین خاص صنعتی و فدرال مطابق باشند، بلکه باید با استانداردهای امنیتی گوناگون که توسط شرکای تجاری آنها وضع می‌شوند هم مطابقت داشته باشند. اگر چه هیچ فشارمستقیمی توسط شرکت غالب برای کسب اقدامات احتیاطی امنیتی خاص به کار برده نمی‌شود، با این اوصاف شرکای تجاری اجبار را درک می‌کنند؛ تاجایی که اقدامات امنیتی اطلاعات آنها تأثیر بالقوه‌ای بر ارتباط آن‌ها با شرکت اصلی دارد ( Tseng, 2008).

می‌توان چنین نتیجه گیری کرد که فشار اجباری عمدتاً از طریق دو منبع اعمال می‌شو : شرکای تجاری و قوانین امنیتی. بنابراین، فرضیه زیر را مطرح می‌کنیم:

- فشار اجباری بر مدیریت امنیت اطلاعات در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد تأثیر دارد.

**فشار هنجاری**

همگنی در بین سازمان‌ها با گذشت زمان تا حدی به انطباق سازمان‌ها با فشار هنجاری نسبت داده می‌شود. احتمال دارد شرکت‌ها رفتار خود را بر اساس عقاید خود درباره آنچه که در میان گروه‌های اجتماعی مناسب قلمداد می‌شود تنظیم کنند و در نتیجه آن روش‌ها و تکنیک‌هایی که منعکس کننده استانداردهای اخیر آن گروه‌ها هستند، اتخاذ کنند. فشار هنجاری می‌تواند از یک گونه‌ای از منابع مثل شرکای تجاری و انجمن‌های حرفه‌ای اعمال شود. چون شرکت‌های درون یک زنجیره ارزشی عموماً اهداف مشترکی را با هم دنبال می‌کنند، یک شرکت در معرض فشار هنجاری ناشی از دیگر اعضای زنجیره ارزشی قرار دارد (Siponen & Vance, 2014).

نوع دیگری از فشار هنجاری، از مشارکت در تجارت و انجمن‌های حرفه‌ای ایجاد می‌شود. قوانین هنجاری درباره رفتار سازمانی از طریق مشارکت فعال در یک ردیف از وقایع مثل کنفرانس‌ها، کارگاه‌ها و برنامه‌های آموزشی سازمان‌یافته توسط انجمن‌های حرفه‌ای و تجاری تعیین و اعلام می‌شوند. این رویدادها شبیه میدان‌هایی برای به اشتراک‌گذاری تجربه درباره روش‌های امنیتی و یادگیری چهارچوب‌ها و استانداردهای امنیتی رایج عمل می‌کنند.

فشار هنجاری عمدتاً از دو منبع ایجاد می‌شود: سرمایه‌گذاری شرکا در امنیت و در معرض اقامات امنیتی قرار گرفتن. بنابراین، فرضیه زیر را مطرح می‌کنیم:

- فشار هنجاری بر مدیریت امنیت اطلاعات در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد تأثیر دارد.

## مدل مفهومی پژوهش

مدل مفهومی تحقیق به بررسی تعیین تأثیر فشار تقلیدی بر مدیریت امنیت اطلاعات، تعیین تأثیر فشار اجباری بر مدیریت امنیت اطلاعات و تعیین تأثیر فشار هنجاری بر مدیریت امنیت اطلاعات می‌پردازد (نمودار شماره ۱).


**نمودار ۱. مدل تحقیق (Source:By author)**

## روش پژوهش

تحقیق حاضر به لحاظ هدف، کاربردی است چون به دنبال بررسی یک مسئله واقعی و دانش تخصصی می‌باشد و می‌تواند نتایج و یافته‌های حاصل از آن برای مدیران در راستای توسعه کنترل امنیت اطلاعات مربوطه مورد استفاده باشد. از نظر روش گردآوری داده‌ها، توصیفی و از نوع همستگی است که با اهداف و فرضیه‌های این تحقیق تطابق دارد. بنابراین، تحقیق حاضر به دلیل آن که تأثیر ابعاد تئوری نهادی بر منابع کنترل امنیت اطلاعات را بررسی می‌نماید، از نظر هدف کاربردی است و از نظر شیوه گردآوری و تحلیل داده‌ها نیز این تحقیق توصیفی و از نوع همبستگی است. همچنین، به لحاظ زمانی نیز این تحقیق از نوع مقطعی می‌باشد.

### جامعه آماری پژوهش

جامعه آماری این تحقیق، کلیه کلینیک‌ها و بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد به تعداد ۱۰ بیمارستان و۳ کلینیک می‌باشد و سطح تحلیل آن سازمان است.

**روش نمونه گیری و حجم نمونه**

در این پژوهش از روش سرشماری برای جمع آوری داده‌ها استفاده شد و داده‌ها از تمام پرسنل واحد فناوری اطلاعات بیمارستان‌ها و کلینیک‌های آموزشی دانشگاه علوم پزشکی شهرکرد جمع‌آوری شد.

**روش‌های گردآوری داده‌ها**

با توجه به اینکه پژوهش حاضر، یک پژوهش میدانی و کاربردی است، بنابراین برای گردآوری داده‌ها از دو روش استفاده گردیده است:

۱) روش بررسی اسناد و مدارک: در این پژوهش ابتدا با رجوع به منابع کتابخانه‌ای و بکارگیری موتورهای جستجوگر در پایگاه‌های داده اینترنتی مرتبط و فیش‌برداری از اسناد و مدارک مرتبط، مبانی نظری و پیشینهٔ تحقیق تدوین شده است.

۲) روش میدانی: ابزار اصلی گردآوری داده‌ها درمرحلهٔ میدانی، استفاده از پرسشنامهٔ بومی سازی شده است.

**پرسشنامه پژوهش**

به منظور جمع آوری داده‌ها، پرسشنامه بومی سازی شده برای پاسخگویی به سؤالات تحقیق تدوین گردیده که برمبنای پرسشنامه استاندارد کاواسوگلو و همکاران (۲۰۱۵) و پرسشنامه ارزیابی کیفیت سیستم مدیریت امنیت با استفاده از ISO27001 طراحی شده است. فراوانی سؤالات پرسشنامه پژوهش در جدول شماره ۱ نمایش داده شده است.

**جدول ۱- فراوانی سوالات پرسشنامه (Source:By author)**

| بُعد | تعداد سوال | منبع |
|---|---|---|
| فشار تقلیدی | ۴ | کاوسگولو و همکاران (۲۰۱۵) |
| فشار اجباری | ۳ | |
| فشار هنجاری | ۳ | |
| مدیریت امنیت اطلاعات | ۵۷ | ISO 27001 |

**روش‌های تجزیه و تحلیل آماری**

تجزیه و تحلیل حاصل از این پژوهش با استفاده از نرم افزارهای آماری SPSS و Smart PLS در دو سطح آمار توصیفی و استنباطی انجام شد. در بخش آمار توصیفی از مشخصه‌های آماری مانند فراوانی، درصد، میانگین و انحراف معیار و در بخش آمار استنباطی از معادلات ساختاری (روش حداقل مربعات جزئی) استفاده شد.

**یافته‌های پژوهش**

نتایج آزمون فرضیات بر اساس اثر مستقیم استاندارد شده و آماره تی در جدول شماره ۲ آمده است.

**جدول ۲. نتایج آزمون فرضیه‌ها (Source:By author)**

| فرضیه‌های پژوهش | آماره t | اثر مسقیم | معناداری | نتیجه فرضیه |
|---|---|---|---|---|
| فشارهای تقلیدی-><مدیریت امنیت | ۱/۸۹ | ۰/۲۹ | p> ۰/۰۵ | رد |
| فشارهای اجباری -><مدیریت امنیت | ۲/۰۸ | ۰/۲۵ | P<۰/۰۵ | تأیید |
| فشار هنجاری -><مدیریت امنیت | ۳/۱۰ | ۰/۳۲ | P<۰/۰۱ | تأیید |

**بررسی فرضیه اصلی**

- ابعاد تئوری نهادی بر مدیریت امنیت اطلاعات در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد تأثیر دارد.

نتایج آزمون فرضیات در جدول شماره ۲ توسط مدل معادلات ساختاری نشان داد از مؤلفه‌های تئوری نهادی دو مؤلفه فشار اجباری و هنجاری با ضرایب ۰/۲۵ و ۰/۳۲ تأثیر مثبت و معناداری بر مدیریت امنیت اطلاعات داشته و توانسته‌اند ۶۲ ٪ از تغییرات مدیریت امنیت اطلاعات در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد را تبیین و پیش‌بینی کنند. در نتیجه فرضیه اصلی به دلیل رد شدن یکی رابطه ها رد شد.

**بررسی فرضیه‌های فرعی**

- فشار تقلیدی بر مدیریت امنیت اطلاعات در بیمارستان های آموزشی دانشگاه علوم پزشکی شهرکرد تأثیر دارد.

نتایج آزمون فرضیات در جدول شماره ۲ توسط مدل معادلات ساختاری نشان داد آماره تی برای این مسیر ۰/۲۹ می‌باشد و مقدار استاندارد شده آن ۱/۸۹ می‌باشد که نشان از رد فرضیه داشته و می‌توان با اطمینان ۹۵٪ عنوان کرد که فشار تقلیدی بر مدیریت امنیت اطلاعات در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد تأثیر معناداری ندارد.

- فشار اجباری بر مدیریت امنیت اطلاعات در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد تأثیر دارد.

نتایج آزمون فرضیات در جدول شماره ۲ توسط مدل معادلات ساختاری نشان داد آماره تی برای این مسیر ۲/۰۸ می‌باشد و مقدار استاندارد شده آن ۰/۲۵ می‌باشد که نشان از تأیید فرضیه داشته و می‌توان با اطمینان ۹۵٪ عنوان کرد که فشار اجباری بر مدیریت امنیت اطلاعات در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد تأثیر دارد.

- فشار هنجاری بر مدیریت امنیت اطلاعات در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد تأثیر دارد.

نتایج آزمون فرضیات در جدول شماره ۲ توسط مدل معادلات ساختاری نشان داد آماره تی برای این مسیر ۳/۱۰ می‌باشد و مقدار استاندارد شده آن ۰/۳۲ می‌باشد که نشان از تأیید فرضیه داشته و می‌توان با اطمینان ۹۵٪ عنوان کرد که فشار هنجاری بر مدیریت امنیت اطلاعات در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد تأثیر دارد.

**بررسی سوال جانبی پژوهش**

- وضعیت مدیریت امنیت اطلاعات در هریک از ابعاد در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد چگونه است؟

**جدول ۳. میانگین وضعیت مدیریت امنیت اطلاعات (Source:By author)**

| ابعاد مدیریت امنیت اطلاعات | میانگین |
|---|---|
| خط مشی امنیت اطلاعات | ۳/۴۱ |
| سازماندهی امنیت اطلاعات | ۳/۹۵ |
| مدیریت دارایی | ۳/۹۲ |
| مدیریت امنیت منابع انسانی | ۳/۹۳ |
| مدیریت امنیت فیزیکی و محیطی | ۳/۵۶ |
| مدیریت عملیات و ارتباطات | ۳/۸۴ |
| مدیریت کنترل و دسترسی به اطلاعات | ۳/۹۷ |
| توسعه و نگهداری سیستم‌ها | ۳/۵۸ |
| مدیریت حوادث و امنیت اطلاعات | ۳/۹۳ |
| مدیریت استمرار و کسب وکار | ۳/۹۵ |
| مدیریت قوانین امنیت | ۳/۷۳ |

جهت تحلیل سوال جانبی با توجه به استفاده از روش سرشماری، از روش میانگین استفاده شد. از آنجا که میانگین همه ابعاد از ۳ بیشتر شد، می‌توان نتیجه گرفت که وضعیت مدیریت امنیت اطلاعات مراکز درمانی آموزشی دانشگاه علوم پزشکی شهرکرد از نظر کارشناسان فناوری اطلاعات این مراکز در وضعیت مطلوب است.

## بحث و نتیجه گیری

در این پژوهش به تعیین تأثیر ابعاد تئوری نهادی بر مدیریت امنیت اطلاعات در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد پرداخته شد. بر این اساس، سعی شد تا در ابتدا مؤلفه‌های مربوط به هر متغیر بر اساس ادبیات نظری و پیشینه پژوهش شناسائی گردد و در ادامه مدل پژوهش حاصل از تأثیر ابعاد تئوری نهادی بر مدیریت امنیت اطلاعات ترسیم شد. جامعه آماری پژوهش شامل کلیه کلینیک‌ها و بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد به تعداد ۱۰ بیمارستان و۳ کلینیک بود. پرسشنامه‌ها در میان تمامی کارکنان واحدهای فناوری اطلاعات بیمارستان‌ها و کلینیک‌های آموزشی دانشگاه علوم پزشکی شهرکرد توزیع شد و در نهایت ۴۵ پرسشنامه گردآوری گردید. میانگین امتیازات هر بیمارستان و کلینیک محاسبه و به عنوان داده نهایی برای تجزیه و تحلیل مورد استفاده قرار گرفت. پرسش‌نامه‌ها از طریق پرسشنامه استاندارد تهیه و بومی سازی شد. جهت سنجش ابعاد تئوری نهادی از پرسشنامه کاوسگولو وهمکاران (۲۰۱۵) و جهت سنجش مدیریت امنیت اطلاعات از پرسشنامه ایزو ۲۷۰۰۱ استفاده شد. روایی صوری پرسشنامه ها بوسیله استاد راهنما و همچنین روایی محتوا بوسیله اساتید گروه مدیریت و تعدادی از

اعضای نمونه آماری تأیید گردید. پس از آن روایی سازه با استفاده از شاخص‌های روایی همگرا و واگرا تأیید و پایایی پرسشنامه توسط شاخص‌های پایایی ترکیبی و آلفای کرونباخ و بارهای عاملی مورد تأیید قرار گرفت.

سنجش متغیرها در پرسشنامه در طیف پنج درجه‌ای لیکرت صورت پذیرفت. تجزیه و تحلیل داده‌ها در دو سطح آمار توصیفی و آمار استنباطی از طریق مدل درونی و بیرونی توسط نرم افزار Smart PLS صورت پذیرفت. نتایج یافته‌های حاصل از تجزیه و تحلیل فرضیه‌های پژوهش نشان داد که دو بُعد فشار اجباری و هنجاری قابلیت پیشبینی ۶۲٪ مدیریت امنیت را در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد دارا هستند.

در تبیین یافته‌های این بخش از پژوهش می‌توان عنوان کرد که نهادهای خارج از بیمارستان به بیمارستان‌های شهرکرد فشار وارد می‌سازند تا آنها را به متابعت از انتظاراتشان در زمینه برقراری امنیت اطلاعات وادار کنند. از این رو آنها می‌توانند با وضع قوانین و در نظر گرفتن مجازات‌های قانونی و از طریق هنجارسازی در جامعه و ایجاد فشار اجتماعی بیمارستان‌ها را به این موضوع تشویق کنند.

**نتایج مربوط به فرضیه‌های فرعی**

- فشار تقلیدی بر مدیریت امنیت اطلاعات در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد تأثیر دارد.

نتایج آزمون فرضیه‌ها نشان از رد فرضیه داشته و می‌توان با اطمینان ۹۵٪ عنوان کرد که فشار تقلیدی بر مدیریت امنیت اطلاعات در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد تأثیر معناداری ندارد. در زمینه مقایسه نتایج این بخش از فرضیه‌ها می‌توان گفت با توجه به اینکه پژوهش‌های اندکی در این زمینه صورت گرفته است، مقایسه نتایج را با محدودیت روبرو ساخته است. با این حال می‌توان نتایج این بخش را همسو با پژوهش کاواسوگولو و همکاران (۲۰۱۵) دانست که از میان ابعاد تئوری نهادی تأثیر فشار تقلیدی بر تغییرات در سرمایه‌گذاری سازمانی در امینت اطلاعات را مورد تأیید قرار نداده است و ناهمسو با پژوهش الکلبانی و همکاران (۲۰۱۶) می‌باشد؛ زیرا تأثیر فشار تقلیدی بر تعهد مدیریت برای اجرای امنیت اطلاعات را تأیید نموده که دلیل این امر می‌تواند متفاوت بودن متغیر وابسته و جامعه آماری باشد.

در تبیین یافته‌های این بخش از پژوهش می‌توان عنوان کرد که اگرچه به نظر می‌رسد فشار تقلیدی جهت رقابت در بین بیمارستان‌ها می‌تواند در برقراری امنیت اطلاعات در بیمارستان‌ها نقش داشته باشد، با این حال در پژوهش حاضر مورد تأیید واقع نشد که البته با میزان اختلاف اندکی این فرضیه رد شده که ممکن است با تکرار در سایر بیمارستان‌ها و یا افزایش تعداد نمونه آماری مورد تأیید واقع شود. با این وجود می‌توان گفت در بین سه بُعد تئوری نهادی، این بُعد قابلیت پیش‌بینی نسبت به دو بُعد دیگر نداشته است و شاید می‌توان دولتی بودن بیمارستان‌ها و عدم وجود رقابت کافی بین آنها را دلیل بر این امر دانست.

- فشار اجباری بر مدیریت امنیت اطلاعات در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد تأثیر دارد.

نتایج آزمون فرضیه‌ها توسط مدل معادلات ساختاری نشان از تأیید فرضیه داشته و می‌توان با اطمینان ۹۵٪ عنوان کرد که فشار اجباری بر مدیریت امنیت اطلاعات در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد تأثیر دارد.

در زمینه مقایسه نتایج این بخش از فرضیات می‌توان گفت نتایج بطور ضمنی همسو با پژوهش کاواسوگولو و همکاران (۲۰۱۵) است که از میان ابعاد تئوری نهادی تأثیر فشار اجباری و هنجاری بر تغییرات در سرمایه گذاری سازمانی در امنیت اطلاعات را مورد تأیید قرار داده است. همچنین، همسو با پژوهش الکلبانی و همکاران(۲۰۱۶) می‌باشد زیرا تأثیر هر سه بُعد تئوری نهادی شامل فشار اجباری را بر تعهد مدیریت برای اجرای امنیت اطلاعات را تأیید نموده است.

در تبیین یافته‌های این بخش از پژوهش می‌توان عنوان کرد که مؤسسات و نهادهای خارج از بیمارستان می‌توانند با وضع قانون و مقرراتی که برای بیمارستان‌ها وضع می‌کنند آنها را به برقراری امنیت اطلاعات تشویق کنند و از طرفی با در نظر گرفتن مجازات‌هایی برای تخلف آنها را برای کاهش ریسک هرگونه خطا و اشتباهی در بیمارستان وادار سازند. این مقررات در جهت حفظ حقوق بیماران وضع شده است که نوعی کنترل رسمی را برا شکل دهی یک رفتار توصیف می‌کند.

- فشار هنجاری بر مدیریت امنیت اطلاعات در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد تأثیر دارد.

نتایج آزمون فرضیه‌ها نشان از تأیید فرضیه داشته و می‌توان با اطمینان ۹۵٪ عنوان کرد که فشار هنجاری بر مدیریت امنیت اطلاعات در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد تأثیر دارد.

در زمینه مقایسه نتایج این بخش از فرضیه‌ها می‌توان گفت که نتایج این بخش بطور ضمنی همسو با پژوهش کاواسوگولو و همکاران (۲۰۱۵) دانست که از میان ابعاد تئوری نهادی، تأثیر فشار اجباری و هنجاری بر تغییرات در سرمایه‌گذاری سازمانی در امنیت اطلاعات را مورد تأیید قرار داده است. همچنین، همسو با پژوهش الکلبانی و همکاران (۲۰۱۶) می‌باشد؛ زیرا تأثیر هر سه بُعد تئوری نهادی شامل فشار هنجاری بر تعهد مدیریت برای اجرای امنیت اطلاعات را تأیید نموده است.

در تبیین یافته‌های این بخش از پژوهش می‌توان عنوان کرد که رعایت حقوق و حفظ حریم شخصی بیماران که شامل عدم بروز و افشای اطلاعات آنان در بیمارستان‌ها می‌باشد را عموم مردم و مدیران سازمان‌های طرف قرارداد بیمارستان‌ها به عنوان یک رفتار پسندیده و الزامی به عنوان یک هنجار در جامعه پزشکی و درمان پذیرفته‌اند. از طرفی اگر بیمارستان یک سازمان در نظر گرفته شود، بیماران مشتریان آن بوده که باید جلب رضایت آنها در جهت حفظ و بقاء در نظر گرفته شود. زمانی که برقراری امنیت اطلاعات در بیمارستان‌ها در بین مردم یک هنجار باشد، بیمارستان‌ها در پی کسب رضایت بیماران سعی در برقراری آن می‌نمایند.

**نتایج مربوط به سوال جانبی پژوهش**

- وضعیت مدیریت امنیت اطلاعات در هریک از ابعاد در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد چگونه است؟

در محیط کسب و کار الکترونیکی به هم پیوسته امروزی، نگرانی‌ها در خصوص امنیت در حال رشد است. استفاده از فناوری اطلاعات، ریسک‌های ویژه را برای سیستم‌های اطلاعات و به خصوص منابع حیاتی و مهم به همراه دارد که به دلیل ماهیت آن می‌باشد. به همین دلیل، امروزه بسیاری از سازمان‌ها به دنبال ایجاد سیستم‌های امنیتی برای جلوگیری از درز اطلاعاتشان به بیرون می‌باشند تا بتوانند کل مجموعه خود را حفظ کنند. امنیت سیستم اطلاعات مانند یک زنجیره است که نقاط قوت آن تحت تأثیر نقاط ضعف قرار می‌گیرند. دانشگاه علوم پزشکی شهرکرد به عنوان یک سازمان دولتی، حجم وسیعی از اطلاعات را در سیستم‌های موجود در سازمان نگهداری می‌کند که به لحاظ اینکه با اطلاعات شخصی، تحصیلی و شغلی افراد مرتبط هستند، حفاظت بالایی را طلب می‌نماید. باید اطمینان یابیم تمامی ریسک‌ها به طور رسمی مشخص شده، رتبه‌بندی شده، مورد نظارت قرار گرفته و از رویداد آنها جلوگیری شده یا از تأثیر آنها کاسته شده است. درپژوهش حاضر سعی بر آن شد تا به کمک استاندارد ISO/ 27001 وضعیت مدیریت امنیت اطلاعات در هر یک از ابعاد دربخش‌های فناوری اطلاعات دانشگاه علوم پزشک شهرکرد مورد ارزیابی قرار گیرد. جهت تحلیل سوال جانبی با توجه به استفاده از روش سرشماری، از روش میانگین استفاده شد. از آنجا که میانگین همه ابعاد از ۳ بیشتر شد، می‌توان نتیجه گرفت که وضعیت مدیریت امنیت اطلاعات مراکز درمانی آموزشی دانشگاه علوم پزشکی شهرکرد از نظر کارشناسان فناوری اطلاعات این مراکز در وضعیت مطلوب است.

**پیشنهادات کاربردی پژوهش**

با توجه به نتایج بدست آمده از این پژوهش، پیشنهادات کاربردی زیر در جهت ارتقای امنیت سیستم‌های اطلاعاتی از طریق دو فشار اجباری و هنجاری ارائه شده است:

در جهت افزایش فشار اجباری در راستای برقرار امنیت اطلاعات پیشنهاد می‌شود:

- دولت می‌تواند با وضع قوانین مرتبط با برقراری امنیت اطلاعات در بیمارستان‌ها فشار اجباری بر آنها را افزایش دهد.
- نظارت مستمر بر عملکرد سیستم‌های اطلاعاتی بیمارستان‌ها توسط دولت و نهاد ناظر می‌تواند مشکلات را شناسایی کرده و در جهت رفع آنها بکوشند.
- استانداردهای امنیتی در مفاد قراردادهای سازمان‌های طرف قرارداد بیمارستان‌ها الزامی می‌باشد.
- پایبندی به اجرای مجازات برای تخلف در زمینه امنیت اطلاعات در بیمارستان‌ها می‌تواند اهمیت موضوع را مشخص نماید.

در جهت افزایش فشار هنجاری در راستای برقرار امنیت اطلاعات پیشنهاد می‌شود:

- حقوق بیماران در زمینه رعایت امنیت اطلاعات و عدم افشای آن برای سایرین به صورت عمومی اطلاع رسانی شود؛ بطوری که عموم مردم از آن مطلع باشند.

- برقراری دوره‌های آموزشی و سمینارها برای کارکنان بیمارستان و ذکر اهمیت امنیت اطلاعات بیماران می‌تواند در این زمینه مفید باشد.
- برخورد قاطع و مشخص مطابق با آیین‌نامه‌های انضباطی با کارکنان متخلف در بیمارستان می‌تواند به تحکیم این هنجار کمک نماید.
- بررسی سابقه بیمارستان‌ها در زمینه امنیت اطلاعات و تخلفات صورت گرفته توسط همکاران و سازمان‌های طرف قرارداد می‌تواند وجود این هنجار را در جامعه پزشکی مشخص کند.
- استفاده از یک سیستم یکپارچه و نظارت بر آن می‌تواند نظارت بر امنیت اطلاعات را در بیمارستان را کنترل نماید.

**پیشنهادهای پژوهشی**

پیشنهادهای پژوهشی ذیل به محققین آینده ارائه می‌شود:

- بررسی مدل پژوهش در بیمارستان‌های سایر استان‌ها.
- بررسی تأثیر فشارهای نهادی بر امنیت سیستم‌های اطلاعاتی در سایر بخش‌های خدماتی مانند بانک‌ها و...
- در نظر گرفتن متغیرهای میانجی احتمالی بر اساس ادبیات نظری پژوهش.
- انجام پژوهش در مقطع دیگری از زمان.

**محدودیت‌های پژوهش**

شکی وجود ندارد که محققان در مسیر انجام پژوهش‌های خود با مشکلات و محدودیت‌هایی مواجه خواهند شد، حتی این احتمال وجود دارد که نتایج پژوهش نیز تحت تأثیر قرار گیرد. شناخت این محدودیت‌ها امکان تفسیر و تعمیم بهتر نتایج پژوهش و همچنین ارتقاء سطح کیفیت پژوهش‌های آینده را امکان پذیر می‌سازد. پژوهش حاضر نیز با محدودیت‌هایی مواجه بوده که در ادامه مورد بحث قرار می‌گیرد.

- نتایج پژوهش به بیمارستان‌های آموزشی دانشگاه علوم پزشکی شهرکرد محدود بوده، لذا می بایست در تعمیم نتایج به سایر بیمارستان‌ها در سایر استان ها احتیاط نمود.
- نتایج پژوهش به مقطع زمانی انجام این پژوهش محدود بوده، لذا مشخص نمی‌باشد که سطح وضعیت متغیرهای پژوهش در بیمارستان‌ها در سایر بازه‌های زمانی نیز مشابه با نتایج این پژوهش باشد یا خیر.
- محدود بودن مقالات و مطالعات تجربی مشابه در زمینه موضوع تحقیق نیز یکی از محدودیت‌های محقق بوده است.
- در نظر گرفتن ابعاد تئوری نهادی به عنوان متغیرهای مستقل بر مدیریت امنیت بر اساس مدل منتخب پژوهشگر.

## مشارکت نویسندگان

تمام نویسندگان به نسبت سهم برابر در این پژوهش مشارکت داشته‌اند.

## تأیید اخلاقی

رضایت کتبی آگاهانه از افراد برای انتشار اطلاعات ناشناس آنها در این مقاله اخذ شده است.

## تعارض منافع

هیچ‌گونه تعارض منافع توسط نویسندگان بیان نشده است.

## References


Das, S., & Mukhopadhyay, A. (2012). Security and Privacy Challenges in Telemedicine. *CSI Communications*.

Eissazadeh, A. A. (2015). *Ranking of key success factors in implementing the Information Security Management System of the General Administration of Ports and Maritime Affairs* International Conference on New Research in Industrial Management and Engineering, Guilan Province. [In Persian]

Guillen, E., Estupiñan, P., Lemus, C., & Ramirez, L. (2010). *Analysis of security requirements in telemedicine networks. In* Proceedings of annual international conference of telecommunications engineering, Colombia.

Kahooei, M., & Abbasi, Z. (2015). Prioritizing factors affecting the security of electronic health information in medical centers. *Information Management*, *2*(12), 162-170. [In Persian]

Kahouei, M., & Abbasi, Z. ( 2015). The Prioritization of Effective Factors on Electronic Health Information Security in Medical Centers. *Health Inf Manage*, *12*(2), 170.

Mehraeen, E., Ayatollahi, H., & Ahmadi, M. (2014). A Study of Information Security in Hospital Information Systems. *Health Information Management*, *10*(6), 779-788. [In Persian]

Parks, C., Chu, H., Xu, L., & Adams, D. A. (2011). *Understanding the drivers and outcomes of healthcare organizational privacy responses* Proceedings of the Thirty Second International Conference on Information Systems, Shanghai.

Sheikh Abu Masoudi, Ruhollah, Kouhi Habibi, S., Ataei, M., & Ismaili, N. (2015). Evaluation of Information Management Systems of Isfahan University of Medical Sciences Using the Standard ISO/IEC 27001. *Information Security Management*, *3*(12), 306-316. [In Persian]

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of organizational information security management. *Journal of Enterprise Information Management*, *27*(5), 644-667.

Siponen, A., & Vance, B. (2014). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487–502.

Tajfar, A. (2014). *Ranking the barriers to implementing information security management systems and assessing the level of exploration management readiness* [Master's thesis, Tabriz.

Tallon, P. P., & Pinsonnault, A. (2011). Competing perspectives on the link between strategic information technology alignment and organizational agility: insights from a mediation model. *MIS Quarterly*, *35*(2), 463-486.

Tseng, S. M. (2008). The effects of Control of information security. on knowledge management systems. *Expert Systems with Applications*(35), 150–160.